

REMARKS

Claims 1-6, 8-12, and 14-23 are pending. No claim amendments are made with this response. Reconsideration of the application is respectfully requested based on the following remarks.

I. REJECTION OF CLAIMS 1-6, 8-12, and 14-23 UNDER 35 U.S.C. § 103(a)

Claims 1-6, 8-12, and 14-23 were rejected under 35 U.S.C. § 103(a), as being unpatentable over U.S. Patent No. US 7,003,118 B1 Yang et al. (Yang) in view of U.S. Patent No. US 6,418,130 B1 Cheng et al. (Cheng). Withdrawal of the rejection is respectfully requested for at least the following reasons.

- i. Neither Yang nor Cheng teach a security system that is adapted to employ an initial random data string from the outgoing data to begin encryption before security association information has been retrieved by the security system, as recited in independent claims 1 and 15.*

Independent claim 1 recites a network interface system that is adapted to obtain initialization vector information from the host system and provide the initialization vector information to the security system, ***wherein the security system is adapted to employ an initial random data string from the outgoing data to begin encryption before security association information has been retrieved by the security system.***

The Office Action dated 4/29/2009 (see page 3, paragraph 5 to page 4 paragraph 1) admits that Yang does not teach “the security system is adapted to employ an initial random data string from the outgoing data to begin encryption before security association information has been retrieved by the security system.” In an attempt to remedy this deficiency, the Office Action states that Cheng illustrates in Fig. 4 that the SA attributes might be transferred from SU_k 105 to SU_{k+1} 110, and that Column 6:45-7:6 of Cheng, states: “the last CBC output block prior to hand-over, which

is used as the initialization vector for encryption of the first IP packet subsequent to hand-over” (O.A., 4/29/2009, page 4, paragraph 1).

However, Cheng relies upon “reusing **previously established security associations** to support these newly formed connections between the MU (mobile unit) and SU_{k+1} . By reusing these previously established security associations, the MU and SU_{k+1} need not go through the time consuming task of renegotiating the security associations (SA’s) each time the MU changes its point of connection (e.g., undergoes hand-over) within the administrative domain.” (Column 3, lines 53-61 of Cheng). Thus, in order to **re-use an SA**, Cheng **must first have previously negotiated** (retrieved) an SA, which can then be re-used in a subsequent hand-over (from one SU to another) or “if the MU becomes disassociated from the administrative domain, for example, by being handed over to a SU which is not associated with the administrative domain” (Column 7, lines 17-26 of Cheng). By contrast, the security system of the present invention **is adapted to begin encryption before security association information has been retrieved.**

That is, Cheng teaches a significantly different methodology, teaching that “the MU establishes a connection with the SU in the administrative domain for **the first time**, wherein the Internet Key Exchange (IKE) negotiates to **establish an SA...**”, and “**the first time** a MU connects to any SU in a given administrative domain, an IKE phase 1 negotiation and an IKE phase 2 negotiation must be accomplished, thereby **establishing** the ISAKMP SA and the IP_{SEC} SAs respectively.” (Column 4, lines 18-28, and Column 7, lines 7-11 of Cheng). However, the security system of the present invention begins encryption before retrieving an SA, without having to wait for the time consuming task of negotiating the initial SA. (See, in one non-limiting example, Applicants’ specification page 5, lines 27-29).

Thus, the clear difference between Cheng and the present invention is that Cheng must first establish an SA before it can be “re-used” to begin encryption, while by contrast, the present invention begins encryption before security association information has been retrieved by the security system, employing an initial random data

string from the outgoing data. Restating this difference, Cheng must first negotiate an SA before encryption, while in the present invention; encryption begins before retrieving an SA. This is a clear advantage, particularly as Cheng states: it is a *time consuming task of renegotiating the security associations*.

For example, and to illustrate this comparison, assume a cell phone or mobile unit (MU) needs to communicate 50 blocks of data with a first tower or first stationary unit (SU1). According to Cheng, the first time the MU is associated with SU1, the SA's are negotiated (established) in the usual time-consuming negotiation manner. Now upon communicating block 37 of the 50 blocks, let's assume the MU becomes disassociated with SU1 and must be handed-over to a second tower or second SU (SU2) to communicate the remaining data blocks 38 thru 50. According to the teaching of Cheng, the MU will then become associated with SU2 by re-using the previously established security associations, which in this case were established with SU1, to avoid the time consuming task of having to renegotiate the SA's as Cheng admits it did the first time. Then, in accordance with Column 6, lines 61-63 of Cheng, *in the last CBC block (block 37), prior to hand-over to SU2, block 37 is used as the initialization vector for encryption of the first IP packet (block 38) subsequent to hand-over*.

Thus, Cheng may be useful for re-using the previously established security associations, after a hand-over, or after an MU has become disassociated to avoid the time consuming task of renegotiating the security associations. However, to avoid having to wait for this same time consuming task during the initial negotiation of the security associations and to immediately begin the initial encryption, the security system of the present invention *is adapted to employ an initial random data string from the outgoing data to begin encryption **before SA information has been retrieved** by the security system*, as recited in claims 1 and 15.

Thus, neither Yang nor Cheng disclose the features recited in claims 1 and 15. Therefore, Applicant respectfully submits that independent claims 1 and 15, and the claims which depend therefrom, respectively, are non-obvious and therefore patentable

over Yang in view of Cheng. Withdrawal of this rejection is therefore respectfully requested.

II. CONCLUSION

For at least the above reasons, the claims currently under consideration are believed to be in condition for allowance.

Should the Examiner feel that a telephone interview would be helpful to facilitate favorable prosecution of the above-identified application, the Examiner is invited to contact the undersigned at the telephone number provided below.

Should any fees be due as a result of the filing of this response, the Commissioner is hereby authorized to charge the Deposit Account Number 50-1733, AMDP763US.

Respectfully submitted,
ESCHWEILER & ASSOCIATES, LLC

By /Thomas G. Eschweiler/
Thomas G. Eschweiler
Reg. No. 36,981

National City Bank Building
629 Euclid Avenue, Suite 1000
Cleveland, Ohio 44114
(216) 502-0600